Safety levels in the electronic identification system used in health service

(Poziomy bezpieczeństwa w systemie identyfikacji elektronicznej w służbie zdrowia)

Sz Jakubowski [1,A,D], A Romaszewski [1,C,F], Z Kopański [1,E], J Strychar [2,B], M Liniarski [2,B], T Kilian [2,A,B]

Abstract – The authors of this article have characterised the safety levels depending on the nature of data they refer to. Additionally, they have stressed the requirements that must be met in order for an access to medical and other official data to be obtained. They have also discussed the procedure of electronic identification systems notification, while simultaneously paying attention to the necessity of creating a register of reliable systems using proven means of electronic identification accepted within the European Union and designed by both public and private entities. Furthermore, they have traced the authentication process, and in particular the one conducted in the health service sector.

Key words - safety levels in the electronic identification system, notification, authentication, health service.

Streszczenie – Autorzy scharakteryzowali poziomy bezpieczeństwa zależne od rodzaju danych, których dotyczą. Podkreślili wymagania jakie muszą być spełnione aby uzyskać dostęp do danych medycznych oraz innych danych z formularzy urzędowych. Omówili procedurę notyfikacji (ang. notification) systemów identyfikacji elektronicznej zwracając uwagę na potrzebę stworzenie listy wiarygodnych systemów posługujących się sprawdzonymi środkami identyfikacji elektronicznej uznawanymi na terenie Unii Europejskiej, opracowanymi przez podmioty publiczne jak i prywatne. Prześledzili proces uwierzytelnienia z uwzględnieniem sektora służby zdrowia.

Słowa kluczowe – poziomy bezpieczeństwa w systemie identyfikacji elektronicznej, notyfikacja, uwierzytelnienie, służba zdrowia.

Author Affiliations:

1. Faculty of Health Sciences, Collegium Medicum, Jagiellonian University
2. Collegium Masoviense – College of Health Sciences, Żyrardów

Authors' contributions to the article:
A. The idea and the planning of the study
B. Gathering and listing data
C. The data analysis and interpretation
D. Writing the article
E. Critical review of the article
F. Final approval of the article

Correspondence to:

Prof. Zbigniew Kopański MD PhD, Faculty of Health Sciences, Collegium Medicum, Jagiellonian University, P. Michałowskiego 12 Str., PL- 31-126 Kraków, Poland, e-mail: zkopanski@o2.pl

Accepted for publication: November 28, 2018.

I. THE IMPORTANCE OF SAFETY LEVELS

The safety levels depend on the nature of data they refer to. In order to obtain medical data one must meet requirements different than the ones needed to obtain data from official records [1]. In accordance with the eIDAS regulation, three safety levels of electronic identification means could be distinguished. While using a given online service requiring a specific safety level, one must provide an access on at least the same level of safety. In specific situations, a person may not need higher safety levels of identification means and a lower level might be enough in order to get an access to the services he/she needs [2]. The abovementioned safety levels in the area of electronic identification systems could be classified as follows [2]:

- low level –with a limited level of confidence as to a person's identity; refers to technical specifications,

norms and procedures used, as a rule, in order to diminish the risk of personating or modifying a given person's identity;

- medium level - provides a medium level of confidence as to a person's identity; refers to technical specifications, norms and procedures used, as a rule, in order to diminish significantly the risk of personating or modifying a given person's identity; higher than low level
- high level - with a high level of confidence as to a person's identity; refers to technical specifications, norms and procedures used, as a rule, in order to prevent the risk of personating or modifying a given person's identity; higher than medium level.

The low security level must involve at least one authentication factor included in the electronic identification system, while the medium and high security levels must involve at least two authentication factors. Security levels are used both in electronic identification systems and in electronic identification means. [2]. In case of low security levels, the legislator provided some leeway for the member states in terms of the outer electronic identification means acceptance. However, reliable low and medium-level identification means must be obligatorily accepted by the EU member states [1,3].

Table 1. Security levels according to the eIDAS regulation

Category/Levels	**Low**	**Medium**	**High**
Access to online services	access only to low-level security services	access to low- or medium-level security services	access to all services
Number of authentication factors included in electronic identification	at least one	two or more	two or more
Personating or identity modification risk	risk lowering	significant risk lowering	risk prevention
Recognition in EU	voluntary	obligatory	obligatory

Due to data sensitivity in health security, it is advisable to use high-level security in electronic identification systems. [4].

II. NOTIFICATION

The procedure of electronic identification systems notification was devised to enable creating a register of reliable systems providing proven means of electronic identification accepted within the European Union and designed by both public and private entities. The objective of such register is to cause an increase in confidence concerning data storage in electronic identification systems. Each member state is entitled to notify to the European Commission its own electronic identification system. Additionally, the European Commission has established a collaborative network, seen as a group of member state representatives, responsible for issuing the assessments of notified systems. A positive notification requires meeting a set of technical, organisational and security demands [2].

III. AUTHENTICATION PROCESS

The result of identification process is identifying a person holding a given ID tag, whereas the process of authentication provides undisputable proof that the person really is the one he/she is claiming to be [1].

A user trying to prove his/her identity provides the electronic identification system with an authentication factor, released after positive verification. Additionally, on higher security levels, apart from electronic means verification, the user's authenticity is verified by means of dynamic authentication system [2].

The authentication process defines the authentication factor, i.e. the factor assigned to a given person with confirmed background and connection. There are three types of authentication factors, namely [5]:

- "authentication factor based on possession- i.e. an authentication factor, in case of which a person subject to authentication process is required to prove such possession;
- authentication factor based on knowledge- i.e. an authentication factor, in case of which a person subject to authentication process is required to prove such knowledge ;

- authentication factor based on inborn qualities - i.e. an authentication factor based on a real attribute of a natural person. In this case a person subject to authentication process is required to prove the possession of that physical quality."

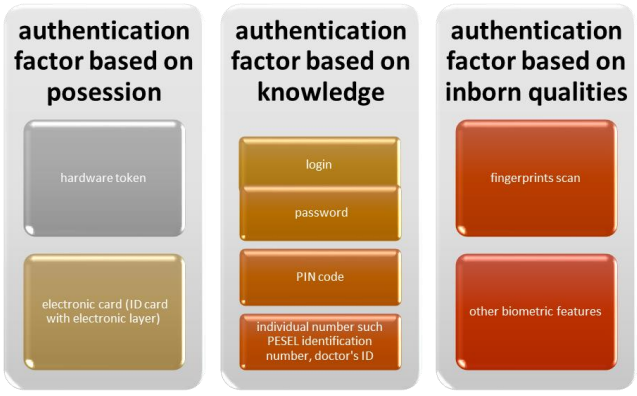

Figure 1. Examples of authentication factors

Additionally, the European legislator has introduced the notion of dynamic authentication, which is "an electronic process using cryptography or other techniques providing, on demand, an electronic proof that the person subject to authentication process is in the possession of identification data or this data remains in this person's control and is changed with each authentication process being performed between the authenticated person and the system of identification of his/her identity." [5].

If the users of electronic information and communication system employed by public benefit purpose entities, including Independent Public Health Care Centres [Samodzielne Publiczne Zakłady Opieki Zdrowotnej- SP ZOZ], wish to use online services, the authentication process must require as follows [6]:

- the use of notified electronic means of identification, relevant to the security level required by the services provided within the framework of these systems, or
- trusted profile ePUAP, or
- data verified by means of qualified certificate for electronic signature" (Art. 20a. 1).

The process of identity confirmation in public entities can be performed with the use of certification systems or identity management and control systems working in compliance with state regulations.

The certification system issues or invalidates certificates used by public entities to authenticate users. The identity management and control system, however, uses methods other than certification while processing data during authentication. *The Ordinance of the Minister of Digitization* of *5 October 2016 on specified organizational and technical conditions that should be met by electronic information and communication system used for authenticating users (Journal of Laws 2016 item. 1627)* specifies technical and safeguarding standards included in both systems and defines their objectives [7] .

IV. REFERENCES

[1] Romaszewski A, Trąbka W, Kielar M, Gajda K. Identyfikacja i uwierzytelnienie w systemie informacyjnym opieki zdrowotnej po wprowadzeniu rozporządzenia UE eIDAS. [Identification and authentication in health care information systems after implementing the EU eIDAS regulation] Zesz Nauk Wyższej Szk Zarządzania Bank W Krakowie [Cracow University, Department of Management and Banking]. 2016;(41):1–23.

[2] Marucha-Jaworska M. Rozporządzenie eIDAS : zagadnienia prawne i techniczne [eIDAS regulation: legal and technical issues]. Warsaw; Wolters Kluwer, Poland, 2017.

[3] Regulation of the European Parliament and the European Council 910/2014 of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC [online] [cited 2018 Mar 18] Available from: URL: https://eur-lex.europa.eu

[4] Centrum Systemów Informacyjnych Ochrony Zdrowia [The Centre of Health Information Systems].: Recommendations of the Centre of Health Information Systems on safety and technological solutions used during medical records processing [online] [cited 2018 Mar 18] Available from: URL: https://www.csioz.gov.pl/aktualnosci/szczegoly/rekomendacje-w-zakresie-bezpieczenstwa-oraz-rozwiazan-technologicznych-stosowanych-podczas-przetw/

[5] The EU Commission.: Appendix "Technical specifications and procedures regarding low, medium and high level of trust as regards the electronic identification means issued as part of notified electronic identification system" to Commission Implementing Regulation (EU) 2015/1502 of 8 September 2015 on minimum technical specifications and procedures related to the levels of trust within the electronic identification means under Art. 8 par.3 of the Regulation of the European Parliament and the European Commission (EU) 910/2014 on electronic identification and trust services for electronic transactions in the internal market [[online] [cited 2018 Mar 18] Available from: URL: https://eur-lex.europa.eu

[6] Act of 17 February 2005 r. on computerisation of the activity of entities performing public tasks (Journal of Laws, 2005 No 64 item 565). [online] [cited 2018 Mar 18] Available from: URL: http://prawo.sejm.gov.pl

[7] The Ordinance of the Minister of Digitization of 5 October 2016 on specified organizational and technical conditions that should be met by electronic information and communication system used for authenticating users (Journal of Laws, 2016 item 1627). [online] [cited 2018 Mar 18] Available from: URL: http://dziennikustaw.gov.pl